



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/525,956

02/28/2005

Itaru Takemura

050088

3072

23850 7590 04/21/2008
KRATZ, QUINTOS & HANSON, LLP
1420 K Street, N.W.
Suite 400
WASHINGTON, DC 20005

EXAMINER

GYORFI, THOMAS A

ART UNIT

PAPER NUMBER

2135

MAIL DATE

DELIVERY MODE

04/21/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/525,956	Applicant(s) TAKEMURA ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
- ☒ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>2/28/05</u> . | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-22 are pending examination.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 2/28/05 has been considered by the examiner.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specification makes frequent reference to an “encryption key for decryption key”, as well as what may be a corresponding “decryption key for decryption key”; however, Examiner was unable to discern if the terms are indicative of a singular key for use in a symmetric encryption algorithm, or instead the terms are indicative to at least one or both keys of a key pair for an asymmetric encryption algorithm (wherein one key is used for encryption and a second, different key is used to decrypt what the first key encrypted, as in a public/private key algorithm).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 10, 11, 15, 16, and 18 recite the limitation "encryption key for decryption key"; as discussed above, there is insufficient antecedent basis for this limitation in the claim. Additionally, claims 11 and 18 also recite the limitation "decryption key for decryption key"; this is similarly indefinite as it cannot be accurately discerned from the specification as to whether this is a singular key or at least one of an asymmetric key pair. For purposes of examination the Examiner has assumed that each limitation refers to a single specific key. Claims 2-9, 12-14, 17, and 19-22 are rejected at least by virtue of their dependencies on claims 1, 11, 16, and 18.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 1-9 and 19-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

9. Claims 1-9 are directed to an information recording medium comprising encrypted contents, wherein the contents comprise audio/visual data and at least one or more corresponding encryption keys necessary to decrypt said audio/visual data. The claims are thus directed toward non-functional descriptive material, which is non-statutory because no requisite functionality is present to satisfy the practical application requirement. See *Diamond v. Diehr*, 450 U.S. 175, 185-86, 209 USPQ 1, 8.

10. Claims 19 and 20 are directed to an information recording program, i.e. software *per se*, which is not recognized as conforming to any of the statutory classes of invention. Similarly, although claims 21 and 22 are directed to a tangible embodiment of the inventions of claim 19 and 20 respectively, both claims 21 & 22 further limit their respective parent claims by reciting that the respective programs contained therein are

merely "read out" by a computer, rather than "executed" by said computer. As a result, claims 21 & 22 as currently written fail to satisfy the practical application requirement: *In re Lowry*, 32 F.3d at 1583-84, 32 USPQ2d at 1035. See also MPEP 2106.01.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claim 15 is rejected under 35 U.S.C. 102(b) based upon a public use or sale of the invention. Any commercially available DVD employing the Content Scramble System (CSS) implemented the limitations of the claim, as evidenced by "The CSS Decryption Algorithm" (hereinafter, "Touretzky").

Regarding claim 15:

Touretzky discloses an information delivery device comprising: a delivery section for delivering contents encrypted utilizing a content encryption key, and content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption key (page 2, 1st paragraph and accompanying illustration; title key/disc key → content key/encryption for decryption key, respectively).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a

whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1-14 and 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitaya et al. (U.S. Patent Application Publication 2002/0150250) in view of Tsuga et al. (U.S. Patent 5,691,972).

Regarding claim 1:

Kitaya discloses an information recording medium comprising: the encryption key for decryption key is different for each of the regions preset for at least controlling the permission and inhibition of playback of the contents (e.g. paragraphs 0115-0119), and a content encryption key and content decryption key (paragraphs 0143-0147).

Although it is well known that DVDs such as those employed by Kitaya (paragraphs 0002-0003) typically have a region code (e.g. Tsuga, col. 2, lines 35-40), Kitaya does not appear to disclose wherein the content encryption keys and content decryption keys correspond to each of the regions where playback is permitted, or combinations thereof. However, Tsuga establishes wherein it would be desirable to indicate on a recording medium which contents, or portions thereof, should be permitted to be played back based in part on the particular region where one is attempting to play the content (Tsuga, all of column 5 through col. 6, line 10; see also the "Country IDs" in Figures 11-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to make the plurality of content encryption and decryption keys decrypt different versions of the movie stored on that disk based on each of the regions where content playback is permitted, or combinations thereof. The motivation for doing so would be to allow a manufacturer to create a single disk from which a player can selectively decrypt the appropriate version of a movie, in accordance with whichever rating system is appropriate for that region (Tsuga, col. 5, lines 5-35).

Regarding claim 11:

Kitaya discloses an information playback device for playing information including contents encrypted utilizing a content encryption key, and a content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption key, comprising: a decryption key storing section storing a decryption key for decryption key for decrypting the content decryption key encrypted by the encryption key for decryption key (paragraph 0122-0128); a content decryption key decrypting section for decrypting the content decryption key by using the decryption key for decryption key (Ibid); a content decrypting section for decrypting the contents by utilizing the content decryption key (paragraphs 0105-0106), and a playback section for playing the decrypted contents, wherein the decryption keys for decryption key is different for at least controlling the permission and inhibition of the content playback (Ibid, and paragraph 0124).

Although it is well known that DVDs such as those employed by Kitaya (paragraphs 0002-0003) typically have a region code (e.g. Tsuga, col. 2, lines 35-40), Kitaya does not appear to disclose wherein the various encryption keys correspond to each of the regions where playback is permitted, or combinations thereof. However, Tsuga establishes wherein it would be desirable to indicate on a recording medium which contents, or portions thereof, should be permitted to be played back based in part on the particular region where one is attempting to play the content (Tsuga, all of column 5 through col. 6, line 10; see also the "Country IDs" in Figures 11-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to make the plurality of content encryption and decryption keys decrypt different versions of the movie stored on that disk based on each of the regions where content playback is permitted, or combinations thereof. The motivation for doing so would be to allow a manufacturer to create

Art Unit: 2135

a single disk from which a player can selectively decrypt the appropriate version of a movie, in accordance with whichever rating system is appropriate for that region (Tsuga, col. 5, lines 5-35).

Regarding claim 2:

Kitaya further discloses wherein the content decryption key is encrypted by the one or more encryption keys for decryption key provided corresponding to the playback device with which the content playback is permitted (paragraphs 0115-0119).

Regarding claim 3:

Kitaya further discloses wherein header information indicating the kind of encryption key for decryption key is further recorded therein (paragraph 0148)

Regarding claim 4:

Kitaya [in view of Tsuga] further discloses wherein the content encryption key and the content decryption key belong to a region where playback is permitted, and are established corresponding to a combination of playback devices with which the content playback is permitted (paragraphs 0120-0127).

Regarding claim 5:

Kitaya further discloses wherein when the content playback in a predetermined playback device is newly revoked, the content encryption key and the content decryption key are renewed to a new key respectively (e.g. paragraphs 0023-0025).

Regarding claims 6 and 13:

Kitaya [in view of Tsuga] further discloses wherein the encryption keys for decryption keys are managed by a key management system using one or more tree structures provided independently for each region (paragraphs 0113-0127).

Regarding claims 7 and 14:

Kitaya [in view of Tsuga] further discloses wherein the encryption keys for decryption key are managed by a key management system employing one or more tree structures for each of the regions in the state in which one encryption key specified for region independently provided to each of the regions is a root and encryption keys specified for playback device provided to each of the playback devices are the leaves (Ibid; see also Figure 3).

Regarding claim 8:

Kitaya further discloses wherein each of the tree structures employs an n-divided tree, where $n \geq 2$ (Ibid).

Regarding claim 9:

See the rejections of claims 7 and 8 above.

Regarding claim 10:

Kitaya discloses an information recording device, comprising: a content encryption key inputting section for establishing and inputting a content encryption key (the content key¹: paragraph 0105); a content decryption key inputting section for establishing and inputting a content decryption key utilized for decrypting the contents encrypted by the content encryption key (Ibid); an encryption key for decryption key selecting section for selecting an encryption key for decryption key (paragraphs 0118-0124); a content encryption section for encrypting the contents

utilizing the content encryption key (paragraphs 0105-0106); a content decryption key encrypting section for encrypting the content decryption key using the encryption key for decryption key (paragraph 0124), and a recording section for recording at least the encrypted contents and the encrypted content decryption key to an information recording medium (paragraphs 0147-0148).

Although it is well known that DVDs such as those employed by Kitaya (paragraphs 0002-0003) typically have a region code (e.g. Tsuga, col. 2, lines 35-40), Kitaya does not appear to disclose wherein the content encryption keys and content decryption keys correspond to each of the regions where playback is permitted, or combinations thereof. However, Tsuga establishes wherein it would be desirable to indicate on a recording medium which contents, or portions thereof, should be permitted to be played back based in part on the particular region where one is attempting to play the content (Tsuga, all of column 5 through col. 6, line 10; see also the "Country IDs" in Figures 11-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to make the plurality of content encryption and decryption keys decrypt different versions of the movie stored on that disk based on each of the regions where content playback is permitted, or combinations thereof. The motivation for doing so would be to allow a manufacturer to create a single disk that can selectively decrypt the appropriate versions of a movie, in accordance with whichever rating system is appropriate for that region (Tsuga, col. 5, lines 5-35).

Regarding claim 12:

Kitaya [in view of Tsuga] further discloses wherein the decryption key storing section stores therein plural kinds of decryption keys for decryption key including decryption keys specified for region established

¹ Even if one were to assume *arguendo* that the content encryption key and content decryption key were not in fact the same thing, as per a symmetric algorithm, one would nevertheless infer the existence of an encryption key merely based on the simple observation that the content is encrypted (paras. 0006-0011).

corresponding to regions where information playback devices belong to, and decryption keys specified for playback device allotted to each of the information playback devices (paragraphs 0118-0124).

Regarding claims 16, 19, and 21:

Kitaya discloses an information recording method and program comprising: establishing a content encryption key and a content decryption key corresponding to at least one region (paragraphs 0105-0106); obtaining an encryption key for decryption key preset in accordance with the selected region (paragraphs 0114-0115); encrypting the contents utilizing the content encryption key (paragraphs 0105-0106); encrypting the content decryption key using the encryption key for decryption key (Ibid); and recording the encrypted contents and the encrypted content decryption key to an information recording medium (Ibid, and paragraph 0115).

Although it is well known that DVDs such as those employed by Kitaya (paragraphs 0002-0003) typically have a region code (e.g. Tsuga, col. 2, lines 35-40), Kitaya does not appear to disclose wherein multiple region codes would exist to select from. However, Tsuga establishes wherein it would be desirable to indicate on a recording medium which contents, or portions thereof, should be permitted to be played back based in part on the particular region where one is attempting to play the content (Tsuga, all of column 5 through col. 6, line 10; see also the "Country IDs" in Figures 11-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to make the plurality of content encryption and decryption keys decrypt different versions of the movie stored on that disk based on each of the regions where content playback is permitted, or combinations thereof. The motivation for doing so would be to allow a manufacturer to create a single disk that can selectively decrypt the appropriate versions of a movie, in accordance with whichever rating system is appropriate for that region (Tsuga, col. 5, lines 5-35).

Regarding claim 17:

Kitaya further discloses establishing the encryption key for decryption key with a combination having the number smallest in a group of the encryption keys for decryption key, in which the encryption keys for decryption key owned by the playback devices being permitted to play in a selected region is included, and the encryption key for decryption key owned by playback device being prohibited from playing is not included (paragraphs 0118-0124).

Regarding claims 18, 20, and 22:

Kitaya discloses an information playback method and program comprising: the decryption key for decryption key is different at least for controlling the permission and inhibition of the content playback (paragraphs 0118-0124); the content encryption key and the content decryption key are established (paragraphs 0105-0106); checking whether or not an information playback device has a decryption key for decryption key corresponding to the encryption key for decryption key encrypting the content decryption key (paragraphs paragraphs 0143-0147); decrypting the content decryption key using the decryption key for decryption key when the information playback device has the corresponding decryption key for decryption key (Ibid); decrypting the contents utilizing the decrypted content decryption key (Ibid, and paragraphs 0105-0106); and playing the decrypted contents (Ibid).

Although it is well known that DVDs such as those employed by Kitaya (paragraphs 0002-0003) typically have a region code (e.g. Tsuga, col. 2, lines 35-40), Kitaya does not appear to disclose wherein the various encryption keys correspond to each of the regions where playback is permitted, or combinations thereof. However, Tsuga establishes wherein it would be desirable to indicate on a recording

medium which contents, or portions thereof, should be permitted to be played back based in part on the particular region where one is attempting to play the content (Tsuga, all of column 5 through col. 6, line 10; see also the "Country IDs" in Figures 11-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to make the plurality of content encryption and decryption keys decrypt different versions of the movie stored on that disk based on each of the regions where content playback is permitted, or combinations thereof. The motivation for doing so would be to allow a manufacturer to create a single disk that can selectively decrypt the appropriate versions of a movie, in accordance with whichever rating system is appropriate for that region (Tsuga, col. 5, lines 5-35).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- U.S. Patent 6,694,023 to Kim
- U.S. Patent 7,269,257 to Kitaya et al.
- U.S. Patent Application Publication 2002/0169971 to Asano et al.
- U.S. Patent Application Publication 2002/0051540 to Glick et al.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
4/1/08
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135